

Cente Technical Information

発行番号	101-0102	Rev	第1版	発行日	2019/04/17
題名	opendir()で“¥¥”を指定後、readdir()で終端まで読み出すとNULLポインタアクセスする不具合について				
情報分類	障害情報				
適用製品	・Cente FileSystem Ver 6.20 ~ Ver 6.40				
影響API	readdir, readdir_uni				
関連資料	なし				

【現象】

以下の手順で実行した場合に、NULLポインタアクセスが発生します。

【発生手順】

- ①opendir()の引数に、“¥¥”を指定し、ディレクトリポインタを取得。
- ②readdir()の引数に、ディレクトリポインタを指定し、繰り返し実行。
- ③ディレクトリポインタが終端の状態、readdir()を実行。

※readdir_uni()使用時も、同様の手順で本症状は発生します。

【原因】

readdir() は、opendir() で取得したディレクトリポインタを基にディレクトリ下を順次読み出す仕様になっているのですが、有効ドライブを全て読み出した状態で readdir() を実行すると、NULLポインタアクセスしてしまう不具合がありました。

本来であれば、ST_DISK構造体“d”(ディレクトリ構造体“dp”のメンバ変数)がNULLになっていることで終端を検出し、APIの戻り値をNULLで返すのが正しい処理内容ですが、NULLチェックを行っていなかったため、“d”をそのまま参照してしまい、NULLポインタアクセスが発生しておりました。

【回避方法】

■プログラムによる回避方法

修正ソースにつきましては、弊社サポートまでお問い合わせ下さい。

以上